Incorrectly configured Forest - or Domain trust

A forest consists of two or more domains.

The domain can have trust between each other. This means that a security principal (a user for example) can access a resource on the other domain. This might be intended.

Previously the forest was viewed as a security boundry. So even though there was bi-directional trust between forests (so called *inter*-forest trust) it was not possible for admins in one forest to take over domain controllers in the other forests. Since the "printer-bug" (MS-RPRN) was discovered by Lee Christensen in 2018 this is not longer the case. This mean that if your organisation has a bi-directional trust with another forest, and that forest gets compromised, it is possible for an attacker to compromise your forest as well.

Type of trust / Direction of trust

The AD can have specific trust types. The types of trusts are the following:

- Parent/Child -
- Cross-link
- External
- Tree-root
- Forest
- MIT

Using Bloodhound

If there is trust between domains in a forrest, it might be that a user is allowed to retrevie

You can just click on the default query "Map domain trusts"

```
MATCH p=(n:Domain)-->(m:Domain) RETURN p
```

How to test for it

You can identify what types of trusts you have by running the following commands:

```
Get-NetForestDomain
Get-NetDomainTrust
```

Get-ADObject -SearchBase "cn=system,dc=evilcorp,dc=se" -Filter * -Properties trustType | where {$_.objectClass –eq "trustedDomain"} | select Name,trustType

Attacking domain trusts

https://posts.specterops.io/not-a-security-boundary-breaking-forest-trusts-cd125829518d?gi=43aabaf65628

Microsofts advistory https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190006